REMARKS

By this Amendment, claims 33-45 are cancelled. Claims 46-58 remain in the application. Thus, claims 46-58 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

Rejection of Claims

I. In item 9 on page 3 of the Office Action, claims 33-45 were rejected under 35 U.S.C. § 102(a) as being anticipated by Woolsey et al. (U.S. 6,029,000). Without intending to acquiesce to this rejection, claims 33-45 have been cancelled in order to expedite allowance of the present application. Accordingly, this rejection is believed to be moot in view of the cancellation of claims 33-45.

II. In item 10 on page 6 of the Office Action, claims 48-51 were rejected under 35 U.S.C. § 102(e) as being anticipated by Kolouch (U.S. 6,694,433). This rejection is respectfully traversed for the following reasons.

A. Claim 48

Claim 48 recites a data processor that is structured by a transmitting data processor and a receiving data processor, where the transmitting data processor is operable to transfer, to the receiving data processor, data to which information for tampering detection is added.

The transmitting data processor of claim 48 is recited as comprising an unprotection list generation unit operable to generate an unprotection list which lists, by type, data that is not to be subjected to tampering detection. Furthermore, the transmitting data processor of claim 48 is recited as comprising a data generation unit operable to generate data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region.

The receiving data processor of claim 48 is recited as comprising an unprotected data authentication unit operable to authenticate, for the data received by the receiver of the receiving data processor, whether the data included in the unprotected data region is

valid based on the unprotection list which has been confirmed as not having been tampered with by the protected data authentication unit of the receiving data processor.

Accordingly, the data processor of claim 48 authenticates whether the data included in the unprotected data region is valid based on the unprotection list which lists, by type, data that is not to be subjected to tampering detection when the protected data authentication unit confirms that the unprotection list has not been tampered with. Therefore, if a data type of data included in the unprotected data region does not coincide with a data type in the unprotection list, the data is determined to be unreliable and is then discarded. As a result, the reliability of data included in the unprotected data region is increased.

Thus, the data processor of claim 48 provides a remarkable and novel effect of increasing the reliability of the data included in the unprotected data region by placing the unprotection list in the protected data region.

Kolouch discloses a XML encryption scheme in which a part of a XML file is encrypted and the remaining part of the XML file is not encrypted. Figure 5 of Kolouch shows that an encrypted object is embedded within another object (see Column 4, lines 53-62 and Column 5, lines 34-42). However, Kolouch does not disclose or suggest the above-described features and effects of the data processor of claim 48. In particular, the encryption scheme of Kolouch does not increase the reliability of an object which is not to be encrypted. In other words, the encryption scheme of Kolouch does not increase the reliability of data included in the unprotected data region, since Kolouch does not authenticate whether data included in the unprotected data region is valid based on the unprotection list which is confirmed as not having been tampered with.

Accordingly, Kolouch clearly does not disclose or suggest each and every limitation or the effects of claim 48 since Kolouch does not disclose or suggest the combination of the unprotected list generation unit, the data generation unit and the unprotected data authentication unit of claim 48.

Therefore, claim 48 is clearly not anticipated by Kolouch since Kolouch fails to disclose each and every limitation of claim 48.

B. Claim 50

Claim 50 recites a data processing method for receiving and processing data to which information for tampering detection is added. The data processing method of claim 50 is recited as comprising receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection. Claim 50 defines that the protected data region includes an unprotection list which lists, by type, the data included in the unprotected data region.

The data processing method of claim 50 is also recited as comprising authenticating, for the data received in the receiving of the data, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with in the operation of detecting whether the data included in the protected data region has been tampered with.

Accordingly, similar to the data processor of claim 48, the data processing method of claim 50 authenticates whether the data included in the unprotected data region is valid based on the unprotection list which lists, by type, data that is not to be subjected to tampering detection when the detecting operation of claim 50 confirms that the unprotection list has not been tampered with. Therefore, if a data type of data included in the unprotected data region does not coincide with a data type in the unprotection list, the data is determined to be unreliable and is then discarded. As a result, the reliability of data included in the unprotected data region is increased.

Thus, similar to the data processor of claim 48, the data processing method of claim 50 provides a remarkable and novel effect of increasing the reliability of the data included in the unprotected data region by placing the unprotection list in the protected data region.

As demonstrated above, the encryption scheme of Kolouch does not increase the reliability of an object which is not to be encrypted. That is, the encryption scheme of Kolouch does not increase the reliability of data included in the unprotected data region, since Kolouch does not authenticate whether data included in the unprotected data region

is valid based on the unprotection list which is confirmed as not having been tampered with.

Accordingly, Kolouch clearly does not disclose or suggest each and every limitation or the effects of claim 50 since Kolouch does not disclose or suggest the combination of the receiving operation and the authenticating operation of claim 50.

Therefore, claim 50 is also clearly not anticipated by Kolouch since Kolouch fails to disclose each and every limitation of claim 50.

C. Claim 51

Claim 51 recites a data processing method for transferring data, to which information for tampering detection is added, from a transmitting data processor to a receiving data processor. The data processing method of claim 51 recites that the transmitting data processor performs operations of generating an unprotection list which lists, by type, data that is not be subjected to tampering detection, and generating data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region.

Furthermore, the data processing method of claim 51 recites that the receiving data processor performs, in part, an operation of authenticating, for the data received in the receiving of the data, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with in the operation of detecting whether the data in the protected data region has been tampered with.

Accordingly, similar to the data processor of claim 48 and the data processing method of claim 50, the data processing method of claim 51 authenticates whether data included in the unprotected data region is valid, based on the unprotection list which has been confirmed as not having been tampered with. Therefore, the data processing method of claim 51 also provides the remarkable and novel effect of increasing the reliability of the data included in the unprotected data region.

As described above, the encryption scheme of Kolouch does not increase the reliability of an object which is not to be encrypted. In other words, the encryption scheme of Kolouch does not increase the reliability of data included in the unprotected data region, since Kolouch does not authenticate whether data included in the unprotected data region is valid based on the unprotection list which is confirmed as not having been tampered with.

Accordingly, Kolouch clearly does not disclose or suggest each and every limitation or the effects of claim 51 since Kolouch does not disclose or suggest the combination of generation operation and the authenticating operation of claim 51.

Therefore, claim 51 is also clearly not anticipated by Kolouch since Kolouch fails to disclose each and every limitation of claim 51.

III. In item 12 on page 9 of the Office Action, claims 46, 52 and 57-58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Woolsey et al. in view of Gong et al. (NPL "Going Beyond the Sandbox: An Overview of The New Security Architecture in The JAVA Development Kit 1.2"). This rejection is respectfully traversed for the following reasons.

A. Claim 46

Claim 46 recites a data processor for receiving and processing data to which information for tampering detection is added. The data processor of claim 46 is recited as comprising a receiver operable to receive data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection. Claim 46 defines that the protected data region includes an unprotection list which lists, by type, the data included in the unprotected data region.

The data processor of claim 46 also comprises an unprotected data authentication unit operable to authenticate, for the data received by the receiver, whether the data included in the unprotected data region is valid based on the unprotection list which has been confirmed as not having been tampered with by the protected data authentication unit of claim 46.

Accordingly, the data processor of claim 46 provides a remarkable and novel effect of increasing the reliability of data included in the unprotected data region since the validity of the data included in the unprotected data region is authenticated based on the unprotection list which has been confirmed as not having been tampered with by the protected data authentication unit.

Woolsey et al. discloses a mobile communication system in which an applet is encrypted. In the mobile communication system of Woolsey et al., a processor downloads, via a network, an applet which has been signed and encrypted, and then verifies whether or not a signature of the applet is valid based on a list of trusted sources. If the signature is determined to be valid, the processor decrypts the encrypted applet (see Column 20, line 50 to Column 21, line 17).

Gong et al. discloses JDK1.1 and JDK1.2 security models. Gong et al. discloses that when an applet is received, the JDK1.1 security model (or JDK1.2 security model) verifies a signature of the applet, and, if the signature is determined to be valid, permits the applet to access resources of a computer having received the applet.

However, neither Woolsey et al. nor Gong et al. disclose or suggest the above-described features and effects of claim 46. That is, Woolsey et al. and Gong et al. do not increase the reliability of data that is not to be encrypted. In other words, Woolsey et al. and Gong et al. do not increase the reliability of data included in an unprotected data region by authenticating the validity of the data included in the unprotected data region based on the unprotection list which has been confirmed as not having been tampered with, as recited in claim 46.

Accordingly, Woolsey et al. and Gong et al., either individually or in combination, clearly fail to disclose or suggest each and every limitation of claim 46 since Woolsey et al. and Gong et al. each fail to disclose or suggest the combination of the receiver and the unprotected data authentication unit of claim 46.

Therefore, no obvious combination of Woolsey et al. and Gong et al. would result in the invention of claim 46 since Woolsey et al. and Gong et al., either individually or in combination, clearly fail to disclose or suggest each and every limitation of claim 46.

Accordingly, claim 46 is clearly patentable over Woolsey et al. and Gong et al.

B. Claim 52

Claim 52 recites a data processor for receiving and processing data with a digital signature. The data processor of claim 52 is recited as comprising a signer certificate acquiring unit operable to acquire a signer certificate indicating, by type, what data is signable by a signer of the data received by the receiver of the data processor of claim 52.

Furthermore, the data processor of claim 52 is recited as comprising a signature authentication unit operable to determine, when the signer certificate acquired by the signer certificate acquiring unit indicates, by type, the data received by the receiver, that a signature applied to the data is valid.

Accordingly, by including the features of the signer certificate acquiring unit and the signature authentication unit, the data processor of claim 52 verifies the validity of a data type of received data, and if the data is determined to be invalid, the received data is determined to be invalid. Thus, only received data whose data type has been determined to be valid is subjected to the verification operation of the signature authentication unit. Since the validity of the data is verified in advance, a processing time and a size of a memory which is required for verifying the validity of the signature are reduced. Consequently, the data processor of claim 52 produces a remarkable and novel effect of reducing overall processing time and the required memory size for verifying the validity of the received data. Moreover, the data processor of claim 52 provides another novel effect in which data types are easily managed by the signer certificate acquiring unit which acquires a signer certificate indicating, by type, what data is signable.

As described above, Woolsey et al. discloses a mobile communication system in which an applet is encrypted. In the mobile communication system of Woolsey et al., a processor downloads, via a network, an applet which has been signed and encrypted, and then verifies whether or not a signature of the applet is valid based on a list of trusted sources. If the signature is determined to be valid, the processor decrypts the encrypted applet (see Column 20, line 50 to Column 21, line 17).

As also describe above, Gong et al. discloses JDK1.1 and JDK1.2 security models. Gong et al. discloses that when an applet is received, the JDK1.1 security model (or JDK1.2 security model) verifies a signature of the applet, and, if the signature is

determined to be valid, permits the applet to access resources of a computer having received the applet.

However, Woolsey et al. and Gong et al. merely disclose conventional techniques regarding JAVA and do not even suggest or contemplate the above-described features and effects of claim 52. In particular, Woolsey et al. and Gong et al., either individually or in combination, do not disclose or suggest a signature authentication unit operable to determine, when the signer certificate acquired by the signer certificate acquiring unit indicates, by type, the data received by the receiver, that a signature applied to the data is valid, as recited in claim 52.

Accordingly, Woolsey et al. and Gong et al., either individually or in combination, clearly fail to disclose or suggest each and every limitation of claim 52 since Woolsey et al. and Gong et al. each fail to disclose or suggest the combination of the signer certificate acquiring unit and the signature authentication unit of claim 52.

Therefore, no obvious combination of Woolsey et al. and Gong et al. would result in the invention of claim 52 since Woolsey et al. and Gong et al., either individually or in combination, clearly fail to disclose or suggest each and every limitation of claim 52.

Accordingly, claim 52 is clearly patentable over Woolsey et al. and Gong et al.

C. Claim 58

Claim 58 recites a data processing method for receiving and processing data with a digital signature. The method of claim 58 is recited as comprising an operation of acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received in a receiving operation of claim 58. Furthermore, the method of claim 58 is recited as comprising an operation of determining, when the signer certificate acquired in the acquiring of the signer certificate indicates the received data by type, that a signature applied to the data is valid.

Accordingly, similar to the data processor of claim 52, the data processing method of claim 58 verifies the validity of a data type of received data, and if the data is determined to be invalid, the received data is determined to be invalid. Thus, only received data whose data type has been determined to be valid is subjected to the validity determination operation of claim 58. Since the validity of the data is verified in advance, a processing time and a size of a memory which is required for verifying the validity of

the signature are reduced. Consequently, the data processing method of claim 58 produces a remarkable and novel effect of reducing overall processing time and the required memory size for verifying the validity of the received data. Moreover, the data processing method of claim 58 provides another novel effect in which data types are easily managed by the signer certificate acquiring operation which acquires a signer certificate indicating, by type, what data is signable.

As described above, Woolsey et al. and Gong et al. merely disclose conventional techniques regarding JAVA and do not even suggest or contemplate the above-described features and effects of claim 58. In particular, Woolsey et al. and Gong et al., either individually or in combination, do not disclose or suggest determining, when the signer certificate acquired in the acquiring of the signer certificate indicates the received data by type, that a signature applied to the data is valid, as recited in claim 58.

Accordingly, Woolsey et al. and Gong et al., either individually or in combination, clearly fail to disclose or suggest each and every limitation of claim 58 since Woolsey et al. and Gong et al. each fail to disclose or suggest the combination of the signer certificate acquiring operation and the signature authentication determination operation of claim 58.

Therefore, no obvious combination of Woolsey et al. and Gong et al. would result in the invention of claim 58 since Woolsey et al. and Gong et al., either individually or in combination, clearly fail to disclose or suggest each and every limitation of claim 58.

Accordingly, claim 58 is clearly patentable over Woolsey et al. and Gong et al.

IV. In item 13 on page 11 of the Office Action, dependent claims 47 and 53-56 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Woolsey et al. in view of Gong et al. and further in view of Kolouch.

As demonstrated above, Woolsey et al. and Gong et al. clearly fail to disclose or suggest each and every limitation of claims 46 and 52. Claim 47 depends from claim 46, and claims 53-56 depend from claim 52.

Similar to Woolsey et al. and Gong et al., Kolouch fails to disclose or suggest the receiver and unprotected data authentication unit of claim 46, and Kolouch fails to disclose or suggest the signer certificate acquiring unit and the signature authentication unit of claim 52.

Therefore, Kolouch does not cure the deficiencies of Woolsey et al. and Gong et al. for failing to disclose each and every limitation of claims 46 and 52.

Accordingly, no obvious combination of Woolsey et al., Gong et al. and Kolouch would result in the inventions of claims 46 and 52 since Woolsey et al., Gong et al. and Kolouch, either individually or in combination, do not disclose or suggest each and every limitation of claims 46 and 52.

Because of the clear distinctions discussed above, it is submitted that the teachings of Kolouch, Woolsey et al. and Gong et al. clearly do not meet each and every limitation of claims 46, 48, 50-52 and 58.

Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Kolouch, Woolsey et al. and Gong et al. in such as manner as to result in, or otherwise render obvious, the present invention as recited in claims 46, 48, 50-52 and 58.

Therefore, it is submitted that the claims 46, 48, 50-52 and 58, as well as claims 47, 49 and 52-57 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

It is noted that the Examiner, in item 7 on page 2 of the Office Action, alleged that the Applicants "admit[ted] the different techniques of digital signatures and partially encrypting information (protected and unprotected data regions) were well known at the time the invention was made." To support this assertion, the Examiner referred to reference "AN" listed on the September 17, 2003 Form PTO-1449 which was not applied by the Examiner in rejecting the claims.

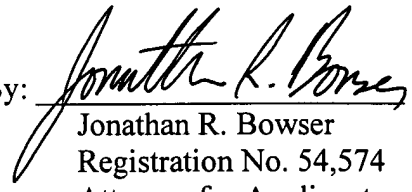
Without acquiescing to this assertion by the Examiner, the Applicants submit that the present invention is clearly patentable over the references applied by the Examiner for the above-described reasons.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Takuya KOBAYASHI et al.

By: 

Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 31, 2006